

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-063063

(43)Date of publication of application : 28.02.2002

(51)Int.CI.

G06F 12/00

G06F 12/14

(21)Application number : 2001-167946

(71)Applicant : FUJITSU LTD

(22)Date of filing : 04.06.2001

(72)Inventor : IWATANI SAWAO

(30)Priority

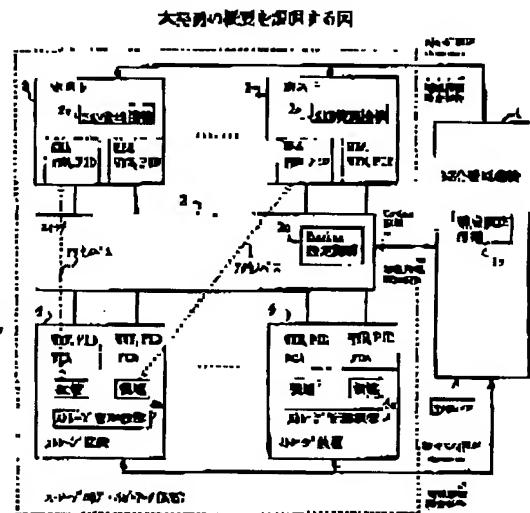
Priority number : 2000167482 Priority date : 05.06.2000 Priority country : JP

## (54) STORAGE AREA NETWORK MANAGING SYSTEM

## (57)Abstract:

**PROBLEM TO BE SOLVED:** To automatically perform best security management for a SAN(storage area network) by unitarily integrating/managing conventional discrete security methods.

**SOLUTION:** An integrating/managing mechanism 1 for integrating/managing SAN is installed, so that access relations between hosts 2 and storage devices 4 can be collectively managed by using the managing mechanism 1. Access paths, that is, areas on the storage device 4 side which are to be accessed from the host 2 side, and fiber channel adaptors(FCAs) and host bus adaptors(HBAs), which are used when the storages are accessed, are set in the mechanism 1. Based on access path information set, the mechanism 1 performs storage settings, a zoning setting, and settings for which area to permit access, for SAN managing mechanism 2a of the hosts 2, a zoning setting mechanism 3a of a switch 3, and storage managing mechanisms 4a of the storage devices 4, respectively.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2002-63063

(P2002-63063A)

(43)公開日 平成14年2月28日(2002.2.28)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テマコート <sup>8</sup> (参考)
G 06 F 12/00	5 4 5	G 06 F 12/00	5 4 5 B 5 B 0 1 7
	5 3 7		5 3 7 A 5 B 0 8 2
12/14	3 2 0	12/14	3 2 0 A

審査請求 未請求 請求項の数9 OL (全20頁)

(21)出願番号	特願2001-167946(P2001-167946)	(71)出願人	000005223 富士通株式会社 神奈川県川崎市中原区上小田中4丁目1番 1号
(22)出願日	平成13年6月4日(2001.6.4)	(72)発明者	岩谷 沢男 神奈川県川崎市中原区上小田中4丁目1番 1号 富士通株式会社内
(31)優先権主張番号	特願2000-167482(P2000-167482)	(74)代理人	100100930 弁理士 長澤 俊一郎 (外1名)
(32)優先日	平成12年6月5日(2000.6.5)		Fターム(参考) 5B017 AA03 BA06 CA07 5B082 EA11
(33)優先権主張国	日本 (JP)		

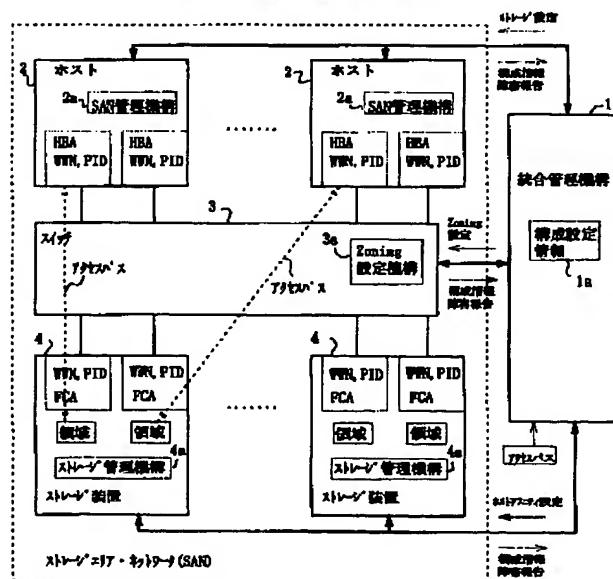
(54)【発明の名称】ストレージエリア・ネットワーク管理システム

(57)【要約】

【課題】 従来の分割されたセキュリティ方式を一元的に統合管理し、SANにおいて最善のセキュリティ管理を自動的に行うこと。

【解決手段】 SANを統合制御する統合管理機構1を設置し、ホスト2とストレージ装置4とのアクセス関係をこの管理機構1を用いて一括して管理できるようする。統合管理機構1にアクセスパス、すなわち、ホスト2側からアクセスをしようとするストレージ装置4側の領域と、そのストレージをアクセスする際の使用するファイバチャネルアダプタ(FCA)、ホストバスアダプタ(HBA)を設定する。設定されたアクセスパス情報を元に、統合管理機構1は、ホスト2のSAN管理機構2a、スイッチ3のゾーニング(Zoning)設定機構3a、ストレージ装置4のストレージ管理機構4aに、それぞれストレージ設定、ゾーニング設定、アクセスをどこの領域に対して許可するかの設定を行う。

本発明の概要を説明する図



**【特許請求の範囲】**

【請求項1】 複数のホストコンピュータと複数のストレージ装置が、スイッチを介して接続されたストレージエリア・ネットワーク・システムにおいて、上記ストレージエリア・ネットワーク・システムを統合制御する統合管理機構を備え、該統合管理機構はホストコンピュータとストレージ装置とのアクセス経路情報を備えるとともに、該アクセス経路情報に基づき、ホストコンピュータのストレージエリア・ネットワーク管理機構に対して、ストレージ装置に対する管理情報を通知し、スイッチの領域設定機構に対して領域情報を通知し、ストレージ装置のストレージ管理機構に対して上記ホストコンピュータについてのアクセス制限情報を通知することを特徴とするストレージエリア・ネットワーク管理システム。

【請求項2】 上記統合管理機構は、ストレージエリア・ネットワークの構成状態を個々の装置より取得して、ストレージエリア・ネットワークの構成設定情報を保持し、

定期的もしくは、システム管理者からの指示によって、現状のストレージエリア・ネットワークの構成状態を集収し、上記構成設定情報を集収した現状の構成情報を比較することにより、ストレージエリア・ネットワーク・システムの異常を判断することを特徴とする請求項1のストレージエリア・ネットワーク管理システム。

【請求項3】 上記統合管理機構は、ホストコンピュータのストレージエリア・ネットワーク管理機構、スイッチ、および／またはストレージ装置より、アクセス関係情報を取得して、アクセスパスの整合性を確認し、アクセスパスが正しく設定されていないとき、その部分を異常として通知することを特徴とする請求項1または請求項2のストレージエリア・ネットワーク管理システム。

【請求項4】 複数のホストコンピュータと複数のストレージ装置が、スイッチを介して接続され、これらを統合管理する統合管理機構を備えたストレージエリア・ネットワーク・システムにおけるホストコンピュータであって、

上記ホストコンピュータのストレージエリアネットワーク管理機構は、上記統合管理機構から通知されるストレージ装置に対する管理情報に基づきストレージ装置に対するアクセス情報を設定することを特徴とするストレージエリア・ネットワーク・システムにおけるホストコンピュータ。

【請求項5】 複数のホストコンピュータと複数のストレージ装置が、スイッチを介して接続され、これらを統合管理する統合管理機構を備えたストレージエリア・ネットワーク・システムにおけるスイッチであって、上記スイッチの領域設定機構は、上記統合管理機構から通知される領域情報に基づき領域設定を行うことを特徴とするストレージエリア・ネットワーク・システムにお

けるスイッチ。

【請求項6】 複数のホストコンピュータと複数のストレージ装置が、スイッチを介して接続され、これらを統合管理する統合管理機構を備えたストレージエリア・ネットワーク・システムにおけるストレージ装置であって、

上記ストレージ装置のストレージ管理機構は、上記統合管理機構から通知されるアクセス制限情報に基づき、ストレージに対するアクセス制限条件を設定することを特徴とするストレージエリア・ネットワーク・システムにおけるストレージ装置。

【請求項7】 複数のホストコンピュータと複数のストレージ装置が、スイッチを介して接続されたストレージエリア・ネットワーク・システムを統合管理する統合管理機構であって、

上記統合管理機構は、ホストコンピュータのストレージエリア・ネットワーク管理機構に対して、ストレージ装置に対する管理情報を通知し、スイッチの領域設定機構に対して領域情報を通知し、ストレージ装置のストレージ管理機構に対して上記ホストコンピュータについてのアクセス制限情報を通知することを特徴とするストレージエリア・ネットワーク・システムにおける統合管理機構。

【請求項8】 複数のホストコンピュータと複数のストレージ装置が、スイッチを介してファイバチャネルで接続されたストレージエリア・ネットワーク・システムを統合制御する統合管理プログラムであって、

上記統合管理プログラムは、ホストコンピュータとストレージ装置とのアクセス経路情報に基づき、ホストコンピュータのストレージエリア・ネットワーク管理機構に対して、ストレージ装置に対する管理情報を通知する処理と、

スイッチの領域設定機構に対して領域情報を通知する処理と、ストレージ装置のストレージ管理機構に対して上記ホストコンピュータについてのアクセス制限情報を通知する処理とをコンピュータに実行させ、

ホストとストレージとのアクセス関係を一括して管理することを特徴とするストレージエリア・ネットワーク・システムを統合制御するプログラム。

【請求項9】 複数のホストコンピュータと複数のストレージ装置が、スイッチを介してファイバチャネルで接続されたストレージエリア・ネットワーク・システムを統合制御する統合管理プログラムを記録した記録媒体であって、

上記統合管理プログラムは、ホストコンピュータとストレージ装置とのアクセス経路情報に基づき、ホストコンピュータのストレージエリア・ネットワーク管理機構に対して、ストレージ装置に対する管理情報を通知し、スイッチの領域設定機構に対して領域情報を通知し、ストレージ装置のストレージ管理機構に対して上記ホストコ

ンピュータについてのアクセス制限情報を通知し、ホストとストレージとのアクセス関係を一括して管理することを特徴とするストレージエリア・ネットワーク・システムを統合制御するプログラムを記録した記録媒体。

#### 【発明の詳細な説明】

##### 【0001】

【発明の属する技術分野】本発明はファイバチャネル・ネットワークを用いて複数のサーバ／複数のストレージを結合するストレージエリア・ネットワーク（以下SANと呼ぶ）の管理システムに関する。

##### 【0002】

【従来の技術】近年、1台のストレージ・システムの容量が大きくなり、複数の多種多様なサーバから使用できるような機能が求められている。また、データ転送経路に高速かつ複数ホスト・ストレージ間の並列転送が可能なファイバチャネルが普及し始めたことをきっかけに、この環境での接続形態はさらに大規模化すると考えられている。このような複数のサーバ／複数のストレージ結合をストレージエリア・ネットワーク（以下SANという）と呼び、分散化されつつある複数サーバのストレージの一元的管理やTOCの削減を計ろうする試みが進みつつある。

##### 【0003】

【発明が解決しようとする課題】しかしながら、ストレージ内の領域管理や、セキュリティの面で解決しなければならない問題がある。その一つに、SANが複数のホストコンピュータ（以下ホストという）及び複数のストレージ・システムより構成されていた場合に、全てのホストから全てのストレージ・システムがアクセス可能である為に、あるホストから使用しているストレージ内のデータが他のホストから不用意に破壊されてしまう可能性があった。

【0004】ストレージ内の領域管理や、セキュリティの面で完全な対策となるものが現状である。また、SANを構成する複数装置で障害が発生した際、いろいろなエラー報告がシステム管理者に報告される為、被疑箇所を特定することが難しく方法がなかった。本発明は上記事情を考慮してなされたものであって、本発明の目的は、従来の分割されたセキュリティ方式を一元的に統合管理し、SANにおいて最善のセキュリティ管理を自動的に行うことのできるようにすることである。

##### 【0005】

【課題を解決するための手段】図1は本発明の概要を説明する図である。同図に示すように、本発明は上記SAN環境に対して、SANを統合制御する統合管理機構1を設置し、ホスト2とストレージ装置4とのアクセス関係をこの管理機構1を用いて一括して管理できるようにする。システム管理者は、統合管理機構1にホスト2側からアクセスをしようとするストレージ装置4側の領域と、そのストレージをアクセスする際の使用するファイ

バチャネル・アダプタ（FCA）、ホストバス・アダプタ（HBA）を設定する。この設定をアクセスパスと呼ぶ。設定されたアクセスパス情報を元に、この統合管理機構1は、まずホスト2側から見えるストレージ設定（Storage affinity）をホスト2側のSAN管理機構2aに設定する。また、スイッチ3のゾーニング（Zoning）設定機構3aに対して、FCA、HBAが保有するWWN、PID情報を事前に確保しておきこれを元に設定されたアクセスパスが実現できるように計算してゾーニング（Zoning）を設定する。さらに、ストレージ装置4のストレージ管理機構4aには、ストレージ装置のどのFCAがどのHBA（WWN、PID）のアクセスをどの領域に対して許可するかの設定を行う。上記のような統合管理機構1を設けることにより、SANにおいて、セキュリティ管理やストレージ内の領域管理を一括して行うことができる。また、上記統合管理機構に、SANの構成状態を構成設定情報1aとして保持させることにより、SANに、SAN管理機能を持たないホストや、ゾーニング設定機能を持たないスイッチや、あるいはストレージ管理機能を持たないストレージ装置が投入されても容易に対応することができ、可能な範囲でセキュリティを確保することができる。

【0006】さらに、上記統合管理機構1を設けることにより、以下の機能を実現することができる。

(1) 統合管理機構1が、SANの構成状態を個々の装置より確保して、構成設定情報1aとして格納し、定期的もしくは、システム管理者からのコマンド指示によって、統合管理機構1が、現状のSANの構成状態を読み、SANの構成設定情報1aと比較し、異なっていた場合は、異常と判断し、システム管理者に通知する。これにより、システム管理者はSANの異常を容易に知ることができる。

(2) 統合管理機構1が、システム管理者からのコマンド指示によって、SAN管理機構2a、Zoning設定機構3a、ストレージ管理機構4aよりアクセス関係情報を確保してアクセスパスの整合性を確認する。アクセスパスが正しく設定されていない場合は、その部分を異常とシステム管理者に通知する。これにより、システム管理者はアクセスパスの整合性を確認することができる。

(3) ホスト2、ホスト2のHBA、スイッチ3、あるいは、ストレージ装置3のFCAが交換されたとき、上記統合管理機構1はこれを検知し、ホスト2のSAN管理機構2a、スイッチ3のゾーニング設定機構3a、もしくは、ストレージ装置4のストレージ管理機構4aから、交換後の設定情報を取得し、交換前と同等のアクセス関係を構築するように再度アクセス関係を設定する。これにより、SANの構成変更に対して容易に対応することができる。

(4) システム起動時にアクセスパスが設定されていな

い状態時に、スイッチ3に対して全てのアクセスを許可しない設定を行う。これにより、システム起動時にアクセスパスを設定していない状態で、不用意なアクセスが設定されることを防ぐことができる。

(5) ファイバチャネルではHBAとFCA側で共通に設定すべきファイバチャネルの転送クラス(Class)というパラメータがある。このパラメータがHBA側とFCA側で異なっていると転送ができない。そこで、前記したアクセスパスを設定する際に、使用する転送クラスもシステム管理者に指定させて、統合管理機構1がSAN管理機構2a、ストレージ管理機構4aを通じて、アクセスパスを設定したHBAとFCAが指定された同一の転送クラスで動作させる。これにより、転送クラスが異なることにより転送できないという不具合を解消することができる。

(6) SAN内で障害が発生した場合は、まず、その障害報告を統合管理機構1が受け取り、システム管理者への報告を一端止める。規定時間他の障害が統合管理機構1が管理している装置から報告されていないかどうかを待ち合わせする。待ち合わせをしている間に受け取った障害報告に関しては中身をチェックし、最初に受け取った障害との関連性がないかを統合管理機構1が保持している各アダプタのWWN、PIDやアクセスパス情報から確認する。確認結果、関連すると判断された場合は、予め統合管理機構1内で設定されている障害報告方法定義に従って、一つのみの障害をシステム管理者に報告する。システム管理者は、この情報を元に迅速に被疑箇所を特定することができる。

(7) 1つの被疑箇所と報告するだけでなく、関連して報告された被疑箇所と判定されなかつた報告も、関連障害として報告する。これにより、影響範囲をシステム管理者は特定することができる。

(8) 予め、統合管理機構1に、各アクセスパスの設定情報だけでなく各アクセスパスで使用しているホスト2側の論理ボリュームの情報もホスト2側のSAN管理機構2aから確保し、統合管理機構1の構成設定情報1aに格納しておく。統合管理機構1は、SAN内から障害が報告されると、その故障箇所を使用しているアクセスパスを統合管理機構1内の構成設定情報1aから取り出し、そのアクセスパスを使用しているホスト論理ボリュームを取り出し、障害影響のある論理ボリュームをシステム管理者に報告する。障害影響のある論理ボリュームが分かると、すぐに、その論理ボリュームのリカバリを行うことができ、業務に対する影響を最小限に止めることができる。

#### 【0007】

【発明の実施の形態】図2に本発明の対象となるSANシステムの構成例を示す。同図に示すように、LAN(ローカルエリア・ネットワーク)に複数台のホストコンピュータ(以下ホストという)H-1~H-nと、後

述するSAN総合管理機構として機能する管理サーバSと、前述したスイッチSW-1~SW-m、ストレージ装置ST、磁気テープ装置MT等が接続される。SAN(ストレージエリア・ネットワーク)は、ホストH-1~H-n、スイッチSW、ストレージ装置ST、磁気テープ装置MT等で構成されており、各ホストH-1~H-n、スイッチSW-1~SW-n、ストレージ装置ST、磁気テープ装置MTの間にはデータ転送路が設けられ、該データ転送路を介して各ホストH-1~H-nからストレージ装置ST等へのアクセスが行われる。また、LANを介してSANの構成状態を示す情報等が管理サーバSに伝送されるとともに、管理サーバSからの各種設定情報等が各ホストコンピュータH-1~H-n、スイッチSW、ストレージ装置ST等に伝送される。

【0008】図3は本発明の実施例のストレージエリア・ネットワーク・システムの構成を示す図である。ここでは、一例としてSANが、ホスト110、120、スイッチ300、ストレージ装置410、420から構成されている場合について説明する。図3において、ホスト110、120はホストバス・アダプタ(以下HBAという)111、112、121を介してファイバチャネルでスイッチ300と接続されており、ストレージ装置410、420はファイバチャネル・アダプタ(以下FCAという)411、412、421を介してスイッチ300と接続されている。図4に図3に示すストレージ装置のハードウェア構成例を示す。同図において、サブシステム制御部11はチャネルI/F部を介して上位装置に接続されており、サブシステム制御部11はメモリ11a、MPU11b、バスインターフェース部11cを備えており、上記MPU11bはメモリ11aに格納されているプログラムに従って動作する。また、メモリ11aには、プログラムの他に、転送データや制御データが格納される。

【0009】13はデバイス制御部であり、デバイス制御部13は、バッファ13a、MPU13b、上記MPU13bを動作させるプログラム等を格納したメモリ13c、バスインターフェース部13dを備えている。上記サブシステム制御部11とデバイス制御部13はバスBUSを介して接続されており、デバイス制御部13はデバイスI/F部14を介してディスクドライブ群15に接続される。

【0010】上記SAN環境に対して、本実施例では、SANを統合制御する管理機構500(前記図2の管理サーバSがこの機能を持つ)を設置し、ホスト110、120とストレージ装置410、420とのアクセス関係をこの管理機構500を用いて一括して管理できるようとする。また、この管理機構500からの制御に対応させる為、ホスト側110、120にはSAN管理機構118、128を設置し、また、ストレージ装置41

0, 420にはストレージ管理機構418, 428を設置する。

【0011】SAN管理機構とは前記a)で説明したストレージ・アフィニティの設定を行える機構であり、ストレージ管理機構は前記したc)で説明したホスト・アフィニティの設定が行える機構である。さらに、スイッチ300には前記b)で説明したスイッチのゾーニング設定機構301が搭載される。システム管理者は、SAN統合管理機構500にホスト側からアクセスをしようとするストレージ側の領域と、そのストレージをアクセスする際の使用するFCA(ファイバチャネル・アダプタ), HBA(ホストバス・アダプタ)を設定する。この設定をアクセスパスの設定と呼ぶ。設定されたアクセスパス情報は、このSAN統合管理機構500の中で、図5(a)に示すSAN統合管理機構500内アクセスパス設定情報の様に格納される。この設定情報を元に、まずホスト側から見えるストレージ設定(Storage affinity)をホスト側のSAN管理機構118, 128に設定する。すなわち、どのHABからどのFCA(WWN, PID)へのアクセスを行うかを設定する。

【0012】また、どのHBAからどのFCAに対してアクセスするかの設定は、図5(b)に示すストレージ・アフィニティ(Storage Affinity)テーブルのような管理テーブルをホスト内で作成し、アクセスするFCAを選択させる事で実現する。この例では、HBA111からWWNcのFCAに対して領域415をアクセスするように設定している。ファイバチャネル上のコマンドは、相手FCAのWWNを介して発行する事が出来る。さらに、スイッチ300のゾーニング(Zoning)設定機構301に対して、FCA, HBAが保有するWWN, PID情報を事前に確保しておき、これを元に設定されたアクセスパスが実現できるように計算してゾーニング(Zoning)を設定する。図5(c)にスイッチ・ゾーニング(Zoning)テーブルの例を示す。ここではゾーン(Zone)をAとBで設定し、それぞれのゾーン(Zone)に相互アクセスを許可するポート(HBA, FCA)の識別子(ここではWWN)を格納する。これにより、スイッチWWNaからアクセスはゾーン(Zone)Aと認識し、WWNcに対してのみしか実行できないようなアクセス制限を行う。

【0013】ファイバチャネル環境ではスイッチ300とポートを接続するとログインシーケンスが動作し、その中でスイッチはポートのWWN情報を確保できる。この情報を元に、ホスト110, 120からストレージ装置410, 420にコマンドが発行された場合に、ゾーン(Zone)設定されていないポートに対するアクセスが指定された時、ストレージ装置410, 420のポートにコマンドが伝わらないような制御を行う。さらに、ストレージ装置410, 420のストレージ管理機構418, 428には、ストレージ装置410, 420のどの

HBA, PIDからのアクセスを、何処の領域に対して許可するかの設定を行う。図5(d)にホスト・アフィニティ(Host affinity)テーブルの例を示す。このテーブルにより、FCA411はWWNaのHBAからのアクセスのみを領域415に対して許可し、FCA412はWWNeのHBAからのアクセスのみを領域416に対して許可する。

【0014】ファイバチャネル環境ではホストからのコマンドを受け付ける前に、ログインシーケンスという相互のポートの情報をやりとりするシーケンスがあり、その中で相手のWWNやPIDなどを確認できる。FCAは、ここで確保した相手のWWNやPIDの情報がアクセス許可されているものかどうかを判断し、アクセス許可がされたものに対してのみ処理を継続し、アクセス許可されていないものからのアクセスに対しては、チェックコンディション(Check condition)等でエラー応答を行う。なお、SANを構成するホスト装置のなかにはSAN管理機構をもたない装置がある。また、ストレージ装置内でも前記c)のホスト・アフィニティ機能を提供していない装置もある。したがって、そのような装置に対して管理機構500はアクセス関係を設定しないが、他のセキュリティ方式(Storage AffinityもしくはZoning)によってセキュリティは保護される。

【0015】図6によりSAN統合管理機構500が行う作業のフローチャートとその作業の具体例を説明する。まず、SAN統合管理機構500は、各FCA, HBAのWWN及びPIDを読み込む(ステップS1)。図3の例においては、SAN統合管理機構500が例えばホスト110のHBA111がWWNa, PIDaであり、ストレージ装置410のFCA411がWWNc, PIDc, FCA412がWWNd, PIDd等であることを認識する。ついで、SAN統合管理機構500は、HBAからアクセスする予定のFCAと、その配下の領域を受け付ける(ステップS2)。図3の例においては、例えばホスト110のHBA111からストレージ装置410のFCA411経由で領域415にアクセスするパス設定を受け付ける。

【0016】次に、当該ホストがストレージ・アフィニティ(Storage Affinity)機能をサポートしているかを調べる(ステップS3)。ストレージ・アフィニティ(StorageAffinity)機能をサポートしていない場合にはステップS5に行く。また、ストレージ・アフィニティ(Storage Affinity)機能をサポートしている場合にはステップS4において、ストレージ・アフィニティ(Storage Affinity)機能により、SAN統合管理機構500は、ホスト側のSAN管理機構に、HBAからアクセスできるデバイスをWWNもしくはPIDを使用して設定する。例えば図3の例においては、ホスト110のHBA111から、ストレージ装置410のFCA411の識別子であるWWNcもしくはPIDcをアクセスできるよう

にS A N管理機構1 1 8に設定する。

【0 0 1 7】ついで、スイッチがゾーニング(Zoning)機能をサポートしているかを調べる(ステップS 5)。ゾーニング機能をサポートしていない場合には、ステップS 7にいく。また、ゾーニング(Zoning)機能をサポートしている場合には、ステップS 6において、スイッチのゾーニング設定機構により、ゾーニング(Zoning)機能をWWNもしくはP I Dを使用して設定する。例えば図3の例においては、ホスト1 1 0のHBA1 1 1から、ストレージ装置4 1 0のF C A 4 1 1へのアクセスはWWN a-WWN cのゾーニング設定、もしくは、P I D a-P I D cのゾーニング設定であり、どちらかをスイッチ3 0 0のゾーニング設定機構3 0 1に設定する。

【0 0 1 8】次に、ストレージ装置がホスト・アフィニティ(Host Affinity)機能をサポートしているかを調べる。ホスト・アフィニティ機能をサポートしていない場合には、処理を終了する。また、ホスト・アフィニティ機能をサポートしている場合には、ステップS 8において、ホスト・アフィニティ機能により、F C Aからアクセスを許可するホスト側のHBAのWWNもしくはP I Dと領域との関係をストレージ装置のストレージ管理機構に設定し、処理を終了する。例えば図3の例においては、ホスト1 1 0のHBA1 1 1のWWN aもしくはP I D aからのコマンドをストレージ装置4 1 0のF C A 4 1 1で受け付けられるように設定し、さらに、WWN aもしくはP I D aからのコマンドに対しては、領域4 1 5をアクセスさせるようにストレージ装置4 1 0のストレージ管理機構4 1 8に設定する。

【0 0 1 9】次に、図7のフローチャートによりスイッチ3 0 0内のゾーニング(Zoning)設定機構3 0 1が行う作業について説明する。まず、ゾーニング(Zoning)設定機構3 0 1をゾーニング(Zoning)設定なしの状態(全てのポート間通信許可モード)に設定する(ステップS 1)。すなわち、標準でゾーンは設定されず、全てのアクセスが許可されるようになる。次に、ゾーニング(Zoning)設定機構3 0 1はS A N統合管理機構5 0 0より、全ポート間通信不許可設定を受け付け(ステップS 2)、全ポート間通信不許可設定とする(ステップS 3)。このように、まず全ポート間通信不許可設定することにより、システム起動時、アクセスパスを設定していない状態で不用意なアクセスが設定されることを防ぐことができる。

【0 0 2 0】ついで、S A N統合管理機構5 0 0より、ゾーン設定(ゾーンを構成するWWN群、もしくは、P I D群)を受け付ける(ステップS 4)。このゾーン設定は例えば、システム管理者がS A N統合管理機構5 0 0を介して行う。上記受け付けたWWN群もしくはP I D群により、ゾーニング(Zoning)設定機構3 0 1に新たなゾーン(Zone)が設定される(ステップS 5)。次にスイッチ3 0 0は、各ポートに接続された相手ポートの

WWNを確保する(ステップS 6)。なお、P I Dはスイッチ3 0 0の物理ポート位置で決まる。ここで、ホストのポートWWN xより相手ポートWWN yへコマンドが発行されると、スイッチ3 0 0は上記コマンド(WWN x→WWN y)を受け付ける(スイッチングS 7)。そして、ゾーニング(Zoning)設定機構3 0 1は、WWN xとWWN yが同一ゾーン(Zone)に設定されているかを調べ(ステップS 8)、同一ゾーンに設定されている場合には、ホストポートより相手ポートに対してコマンドを通過させる。すなわち、スイッチ3 0 0のネームサーバ機能を用いて相手ポートを認識できるようにする(ステップS 9)。また、同一ゾーンに設定されていない場合には、コマンドを通過させない。すなわち、スイッチ3 0 0のネームサーバ機能を用いて相手ポート認識を削除する(ステップS 10)。

【0 0 2 1】次に、上記S A N環境下におけるホストの入出力処理(I/Oオペレーション)の概要について説明する。以下、前記図3によりホスト1 1 0, 1 2 0からI/Oオペレーションが発行された場合の処理例を説明する。なお、ここでは、ホスト1 1 0からHBA1 1 1、スイッチ3 0 0、F C A 4 1 1を経由して、ストレージ4 1 0へのI/Oを行う場合について説明する。まず、ホスト1 1 0は、前記図5(b)に示したストレージ・アフィニティ(Storage Affinity)テーブルより、領域4 1 5のアクセスはHBA1 1 1経由のWWN cを持ったF C Aにアクセスする必要があるということを認識する。ホスト1 1 0はこの情報を元にHBA1 1 1スイッチ3 0 0に対しWWN cに対するI/Oとしてファイバチャネルフレーム発行する。

【0 0 2 2】スイッチ3 0 0はHBA1 1 1より受け取ったWWN cに対するI/Oのファイバチャネルフレームを確保し、HBA1 1 1のWWN aとWWN cが、前記図5(c)のスイッチ・ゾーニング(Zoning)テーブル上同一ゾーン(Zone)であることからアクセスを許可し、WWN cの値が設定されているF C A 4 1 1に対してファイバチャネルフレームを転送する。F C A 4 1 1は受け取ったファイバチャネルフレームが、前記図5(d)のホスト・アフィニティ(Host affinity)テーブル内に設定されているWWN aから来たものと認識できるので、これを処理することが可能と判断し、I/Oを実行する。

【0 0 2 3】次に上記S A N統合管理機構5 0 0が有する各種機能について説明する。

(1) S A N構成設定情報との比較によるシステムの異常検出

前記したように、S A N統合管理機構5 0 0はS A Nの構成情報を個々の装置より確保して、S A Nの構成設定情報5 0 1を格納する。また、S A N統合管理機構5 0 0は、定期的にもしくは、システム管理者からのコマンド指示によって、現状のS A Nの構成情報を読み込み、S

ANの構成設定情報501と比較して、異なっていた場合は、異常と判断してシステム管理者に通知する。例えば、前記図3の状態時にSANの構成設定情報501を登録し、その後ストレージ420の電源が落ちてしまった場合は、SANの構成状態異常と判断して、システム管理者にストレージ420が見えなくなっていることを通知する。

#### 【0024】(2) アクセスパスの整合性の確認

SAN統合管理機構500は、システム管理者からのコマンド指示によって、SAN管理機構118, 128、ゾーニング(Zoning)設定機構301、ストレージ管理機構418, 428よりアクセス関係情報を確保してアクセスパスの整合性を確認する。アクセスパスが正しく設定されていない場合は、その部分を異常とシステム管理者に通知する。この機能によりシステム管理者が勝手に個々の機器の設定を変えてしまった場合に、異常点を検出することが可能となる。また、既に、SANがアクセスパスの設定がされた状態で存在し、新たに当該SAN管理論理を組み込む際に、既存のSANのアクセスパスが正しく設定されているかチェックすることができる。

#### 【0025】(3) HBAの交換時のアクセス関係の再設定

ホスト110側のHBA111が故障して新たなHBAに交換された場合、SAN管理機構118はHBA交換を検知して、システム管理者に通知する。システム管理者からの構成再設定コマンドによって、SAN管理機構118はSAN統合管理機構500に交換された新しいHBAのWWNを伝える。SAN統合管理機構500はその新しいWWNを用いてHBA交換前と同等のアクセス関係を構築し、二つのアクセス関係を設定する機構〔ゾーニング(Zoning)設定機構301、ストレージ管理機構418〕に再度アクセス関係を設定する。

#### 【0026】(4) ホスト交換時のアクセス関係の再設定

ホスト110が故障して新たなホストに交換された場合に、ホスト110のSAN管理機構118は設定がなくなっている事を検知して、システム管理者に通知する。システム管理者からの構成再設定コマンドによって、SAN管理機構118はSAN統合管理機構500に接続されているHBAのWWNを伝え、SAN統合管理機構500は、そのWWNを用いてHBA交換前と同等のアクセス関係を構築し、二つのアクセス関係を設定する機構〔ゾーニング(Zoning)設定機構301、ストレージ管理機構418〕に再度アクセス関係を設定する。

#### 【0027】(5) スイッチ交換時のアクセス関係の再設定

スイッチ300が故障して交換された際に、スイッチに設定したゾーニング(Zoning)情報がなくなっている事を検出し、システム管理者に通知する。SAN統合管理

機構500に、システム管理者からの構成再設定コマンドによって、新しいスイッチに故障前のアクセス関係をセットさせる機構を設け、このような場合に、SAN統合管理機構500から、新しいスイッチに故障前のアクセス関係を再設定する。なお、スイッチ300が故障して交換された際に、スイッチに設定したゾーニング(Zoning)情報がなくなっている事を検出するが、システム管理者には通知せず、自動的にSAN統合管理機構500から新しいスイッチに故障前のアクセス関係をセットさせる機構をSAN統合管理機構500に設け、再設定できるようにしてもよい。

#### 【0028】(6) FCA交換時のアクセス関係の再設定

ストレージ装置側410のFCA411が故障し交換され、FCA側のWWNが変更されてしまった場合に、これを検出しシステム管理者に通知する。システム管理者からの構成再設定コマンドによって、ストレージ管理機構418が新しいFCAのWWNを検出してSAN統合管理機構500に伝え、SAN統合管理機構500はその新しいWWNを用いてFCA交換前と同等のアクセス関係を構築し、二つのアクセス関係を設定する機構〔SAN管理機構118、ゾーニング(Zoning)設定機構301〕に再度アクセス関係を設定する。

#### 【0029】(7) 不用意なアクセスの設定の防止

前述したように、システム起動時にアクセスパスを設定していない状態で、不用意なアクセスが設定されることを防ぐ為に、システム起動時にアクセスパスが設定されていない状態時に、スイッチに対して全てのアクセスを許可しない設定を行う。このような設定がないと、全てのSANのストレージに対して全てのホストからアクセス出来てしまい、セキュリティ上の問題が生ずることがある。

#### (8) ファイバチャネルの転送クラスの設定

ファイバチャネル(FC)ではHBAとFCA側で共通に設定すべきFCの転送クラス(Class)というパラメータがある。転送クラスにはクラス1～3があり、転送クラス1は殆ど使用されず、転送クラス2は転送後、アクノリッジを返し、転送クラス3は転送後、アクノリッジを返さない転送方式である。このパラメータがHBA側とFCA側で異なっていると転送ができない。そこで、前記したアクセスパスを設定する際に、使用するClassもシステム管理者に指定させて、管理機構500がSAN管理機構118, 128、ストレージ管理機構418, 428を通じて、アクセスパスを設定したHBAとFCAが指定された同一のClassで動作させるようとする。

【0030】次に、上記SAN統合管理機構500を用いたSANの障害監視について説明する。基本的にSAN統合管理機構500を用いた場合は、SANを構成する装置(ホスト、スイッチ、ストレージ装置)で発生し

た障害については、装置側から SAN 統合管理機構 500 が装置故障の報告を一括して受け取り、それをシステム管理者に報告する手法をとる。しかし、図 8 に示すように、FCA411 で障害が発生した場合、ストレージ装置 410 より、FCA411 が故障したという報告が SAN 統合管理機構 500 になされるだけでなく、スイッチ 300 からも FCA411 か、FCA411 に接続するスイッチポートが異常であるという報告、ホスト 110 側からの HBA111 からのアクセスパスが使用できないという報告が入ってくる。従って、これらの 3箇所の障害報告をまとめて、一つの報告としてシステム管理者に報告する手法が必要であり、以下では、この手法について説明する。

【0031】SAN 内で障害が発生した場合は、まず、その障害報告を SAN 統合管理機構 500 が受け取り、システム管理者への報告を一端止める。すなわち、規定時間（例えば 1 分間）他の障害が SAN 統合管理機構 500 が管理している装置から報告されていないかどうかを待ち合わせする。待ち合わせをしている間に受け取った障害報告に関しては中身をチェックし、最初に受け取った障害との関連性がないかを SAN 統合管理機構 500 が保持している各アダプタの WWN、PID や前記したアクセスパス情報から確認する。確認の結果、関連すると判断された場合は、予め SAN 統合管理機構 500 内で設定されている図 9 に示すような障害報告方法定義に従って、一つのみの障害をシステム管理者に報告し、この情報を元にシステム管理者は迅速な被擬箇所の特定を行うことができる。

【0032】図 9 に上記障害報告方法定義の一例を示す。同図において、左側の欄は SAN 統合管理機構 500 が受け取った障害情報を示し、右側の欄は SAN 総合管理機構 500 が行う障害報告内容を示す。例えば、

「FCA 自己エラー」と、「スイッチポートアクセスエラー」と「ホスト側アクセスエラー」という障害情報を受け取った場合、SAN 総合管理機構 500 は障害報告方法定義に従い、「FCA 自己エラー」と判断して、障害報告を行う。

【0033】以下、図 10 のフローチャートにより、SAN 統合管理機構が行う SAN の障害監視機能と、FCA411 障害報告方法の例について説明する。まず、SAN 統合管理機構 500 が、障害報告を受け取る（ステップ S1）。例えば、FCA411 に障害が発生した場合、SAN 統合管理機構 500 は、ストレージ装置 410 より FCA411 の障害報告を受け取る。これにより、SAN 統合管理機構 500 は、他の装置からの障害報告があるかどうかを一定時間待ち合わせる（ステップ S2）。スイッチ側から障害報告を受け取ると（ステップ S3）、新たな障害報告の内容と、先ほどの障害報告とのすり合わせを、WWN 等の関連情報から行う（ステップ S4）。例えば、スイッチ 300 から WWN c、P

IDc のバスでエラー発生の報告を受け取ると、WWN c、PIDc が FCA411 のものであるため、SAN 統合管理機構 500 は、同一障害であると認識する。

【0034】次に、ホスト側からの障害報告を受け取ると（ステップ S5）、新たな障害報告の内容と先ほどの障害報告の内容とのすり合わせを WWN 等の関連情報から行う（ステップ S6）。例えば、ホスト 110 から WWNa、PIDa のバスでエラー発生の報告を受けると、WWNa、PIDa と WWNc、PIDc はアクセスパス 600 で連携されていることを SAN 統合管理機構 500 は認識しているため、同一障害と認識する。上記待ち合わせを一定時間行い（ステップ S7）、一定時間待ち合わせると、関連情報をすり合わせた結果、障害の根本原因を特定する（ステップ S8）。根本原因の特定方法は SAN 統合管理機構 500 に含まれる前記障害報告定義によって行われる。例えば、スイッチ 300 側の障害とホスト側の障害は、上記障害報告定義により、ストレージ側の FCA 障害と判断する。

【0035】根本原因が特定されると、根本原因のみをシステム管理者に報告する（ステップ S9）。例えば、前記した FCA411 障害の場合には、FCA411 障害のみをシステム管理者に報告する。上記説明では、被擬箇所を報告するだけであったが、これだけでなく、関連して報告された被擬箇所と判定されなかった報告も、関連障害として報告するようにしてもよい。これにより、影響範囲をシステム管理者は特定できることとなる。

【0036】また、予め、SAN 統合管理機構 500 が、各アクセスパスの設定情報だけでなく各アクセスパスで使用しているホスト側の論理ボリュームの情報もホスト側の SAN 管理機構 118 から確保し、SAN 構成設定情報 501 に格納しておけば、障害影響のある論理ボリュームをシステム管理者に報告することができる。すなわち、SAN 統合管理機構 500 は、SAN 内から障害が報告されると、その故障箇所を使用しているアクセスパスを SAN 統合管理機構 500 内の SAN 構成設定情報 501 から取り出す。さらに、そのアクセスパスを使用しているホスト論理ボリュームを取り出し、障害影響のある論理ボリュームをシステム管理者に報告する。例えば、FCA411 障害の場合には、領域 415 は使用不可であることを報告する。システム管理者は、障害影響のある論理ボリュームがわかると、すぐさまその論理ボリュームのリカバリが可能であり、業務影響を最小限にさせることができるものである。

【0037】（付記 1）複数のホストコンピュータと複数のストレージ装置が、スイッチを介して接続されたストレージエリア・ネットワーク・システムにおいて、上記ストレージエリア・ネットワークを統合制御する統合管理機構を備え、該統合管理機構はホストコンピュータとストレージ装置とのアクセス経路情報を備えること

もに、該アクセス経路情報に基づき、ホストコンピュータのストレージエリア・ネットワーク管理機構に対して、ストレージ装置に対する管理情報を通知し、スイッチの領域設定機構に対して領域情報を通知し、ストレージ装置のストレージ管理機構に対して上記ホストコンピュータについてのアクセス制限情報を通知することを特徴とするストレージエリア・ネットワーク管理システム。

(付記2) 上記統合管理機構は、ストレージエリア・ネットワークの構成状態を個々の装置より取得して、ストレージエリア・ネットワークの構成設定情報として保持し、定期的もしくは、システム管理者からの指示によって、現状のストレージエリア・ネットワークの構成状態を集収し、上記構成設定情報と集収した現状の構成情報を比較することにより、ストレージエリア・ネットワーク・システムの異常を判断することを特徴とする付記1のストレージエリア・ネットワーク管理システム。

(付記3) 上記統合管理機構は、ホストコンピュータのストレージエリア・ネットワーク管理機構、スイッチ、および／またはストレージ装置より、アクセス関係情報を取得して、アクセスパスの整合性を確認し、アクセスパスが正しく設定されていないとき、その部分を異常として通知することを特徴とする付記1または付記2のストレージエリア・ネットワーク管理システム。

(付記4) 複数のホストコンピュータと複数のストレージ装置が、スイッチを介して接続されたストレージエリア・ネットワーク・システムであって、上記ストレージエリア・ネットワークを統合制御する統合管理機構を備え、該統合管理機構はホストコンピュータとストレージ装置とのアクセス経路情報を備えるとともに、該アクセス経路情報に基づき、ホストコンピュータのストレージエリア・ネットワーク管理機構に対して、ストレージ装置に対する管理情報を通知し、スイッチの領域設定機構に対して領域情報を通知し、ストレージ装置のストレージ管理機構に対して上記ホストコンピュータについてのアクセス制限情報を通知するストレージエリア・ネットワーク管理システムにおいて、ホストコンピュータ、ホストコンピュータに設けられたホストバス・アダプタ、スイッチ、あるいは、ストレージ装置に設けられたファイバチャネル・アダプタが交換されたとき、上記統合管理機構はこれを検知し、上記ホストコンピュータのストレージエリア・ネットワーク管理機構、スイッチの領域設定機構、もしくは、ストレージ装置のストレージ管理機構から、交換後の設定情報を取得し、交換前と同等のアクセス関係を構築するように再度アクセス関係を設定することを特徴とするストレージエリア・ネットワーク・システム。

(付記5) ホストコンピュータのホストバス・アダプタが故障して交換された際、統合管理機構はホストバス・アダプタの交換を検知して、システム管理者に通知し、

システム管理者からの構成再設定コマンドにより、統合管理機構1は、ホストコンピュータのストレージエリア・ネットワーク管理機構に交換された新しいホストバス・アダプタの設定情報を伝え、該新しい設定情報を用いてホストバス・アダプタ交換前と同等のアクセス関係を構築し、ストレージエリア・ネットワーク管理機構、領域設定機構、ストレージ管理機構に再度アクセス関係を設定することを特徴とする付記4記載のストレージエリア・ネットワーク・システム。

(付記6) ホストコンピュータが故障して交換された際、統合管理機構は、ホストコンピュータのストレージエリア・ネットワーク管理機構の設定がなくなっている事を検知して、システム管理者に通知し、システム管理者からの構成再設定コマンドにより、上記ストレージエリア・ネットワーク管理機構は統合管理機構に対して接続されているホストバス・アダプタの設定情報を伝え、統合管理機構はその情報を用いてホストコンピュータ交換前と同等のアクセス関係を構築し、領域設定機構、ストレージ管理機構に再度アクセス関係を設定することを特徴とする付記4記載のストレージエリア・ネットワーク・システム。

(付記7) スイッチが故障して交換された際、統合管理機構は、スイッチに設定した領域設定情報がなくなっている事を検出し、システム管理者に通知し、システム管理者からの構成再設定コマンドによって、新しいスイッチに故障前のアクセス関係をセットさせ、アクセス関係を再設定できるようにしたことを特徴とする付記4記載のストレージエリア・ネットワーク・システム。

(付記8) スイッチが故障して交換された際に、スイッチに設定した領域設定情報がなくなっている事を検出し、統合管理機構は、自動的に新しいスイッチに故障前のアクセス関係をセットさせ、アクセス関係を再設定できるようにしたことを特徴とする付記4記載のストレージエリア・ネットワーク・システム。

(付記9) ストレージ装置側のファイバチャネル・アダプタ交換され、ファイバチャネル・アダプタの設定情報が変更された場合、統合管理機構は、これを検出し、システム管理者に通知し、システム管理者からの構成再設定コマンドによって、ストレージ管理機構が新しい設定情報を統合管理機構に伝え、統合管理機構はその新しい設定情報を用いて交換前と同等のアクセス関係を構築し、ストレージエリア・ネットワーク管理機構、領域設定機構に再度アクセス関係を設定することを特徴とする付記4記載のストレージエリア・ネットワーク・システム。

(付記10) 複数のホストコンピュータと複数のストレージ装置が、スイッチを介して接続されたストレージエリア・ネットワーク・システムであって、上記ストレージエリア・ネットワークを統合制御する統合管理機構を備え、該統合管理機構はホストコンピュータとストレ

ジ装置とのアクセス経路情報を備えるとともに、該アクセス経路情報に基づき、ホストコンピュータのストレージエリア・ネットワーク管理機構に対して、ストレージ装置に対する管理情報を通知し、スイッチの領域設定機構に対して領域情報を通知し、ストレージ装置のストレージ管理機構に対して上記ホストコンピュータについてのアクセス制限情報を通知するストレージエリア・ネットワーク管理システムにおいて、システム起動時であって、アクセス経路情報が設定されていない状態の時に、上記統合管理機構はスイッチの領域設定機構に対して全てのアクセスを許可しない設定を行い、その後スイッチの領域設定機構に対して領域設定を行うことを特徴とするストレージエリア・ネットワーク・システム。

(付記11) 複数のホストコンピュータと複数のストレージ装置が、スイッチを介して接続されたストレージエリア・ネットワーク・システムであって、上記ストレージエリア・ネットワークを統合制御する統合管理機構を備え、該統合管理機構はホストコンピュータとストレージ装置とのアクセス経路情報を備えるとともに、該アクセス経路情報に基づき、ホストコンピュータのストレージエリア・ネットワーク管理機構に対して、ストレージ装置に対する管理情報を通知し、スイッチの領域設定機構に対して領域情報を通知し、ストレージ装置のストレージ管理機構に対して上記ホストコンピュータについてのアクセス制限情報を通知するストレージエリア・ネットワーク管理システムにおいて、上記統合管理機構は、指定されたファイバチャネルの転送クラスを、アクセス経路情報を設定したホストコンピュータのストレージエリア・ネットワーク管理機構、ストレージ装置のストレージ管理機構を介して設定し、ホストコンピュータのホストバス・アダプタ、ストレージ装置のファイバチャネル・アダプタを同一の転送クラスで動作させることを特徴とするストレージエリア・ネットワーク・システム。

(付記12) 複数のホストコンピュータと複数のストレージ装置が、スイッチを介して接続されたストレージエリア・ネットワーク・システムであって、上記ストレージエリア・ネットワークを統合制御する統合管理機構を備え、該統合管理機構はホストコンピュータとストレージ装置とのアクセス経路情報を備えるとともに、該アクセス経路情報に基づき、ホストコンピュータのストレージエリア・ネットワーク管理機構に対して、ストレージ装置に対する管理情報を通知し、スイッチの領域設定機構に対して領域情報を通知し、ストレージ装置のストレージ管理機構に対して上記ホストコンピュータについてのアクセス制限情報を通知するストレージエリア・ネットワーク管理システムにおいて、ストレージエリア・ネットワーク・システム内で障害が発生した際、上記統合管理機構は、障害報告を受け取り、規定時間の間、他の障害が報告されているか否かを待ち合わせ、その間に受け取った障害報告をチェックして、最初に受け取った障

害報告との関連性を調べ、関連性があると判断されたとき、予め上記統合管理機構内で設定されている障害報告方法定義に従って、1つの障害箇所のみを報告することを特徴とするストレージエリア・ネットワーク・システム。

(付記13) 1つの障害箇所に加えて、受け取った関連する障害報告を関連障害として報告することを特徴とする付記12記載のストレージエリア・ネットワーク・システム。

(付記14) 上記統合管理機構は、各アクセス経路情報の設定情報に加えて、各アクセスパスで使用しているホスト側の論理ボリュームの情報をホストコンピュータのストレージエリア・ネットワーク管理機構から取得して保持し、ストレージエリア・ネットワーク・システム内から障害が報告されたとき、該障害箇所を使用しているアクセス経路情報に基づき、該アクセスパスを使用している論理ボリュームを取り出し、障害影響のある論理ボリュームを報告することを特徴とする付記12記載のストレージエリア・ネットワーク・システム。

(付記15) 複数のホストコンピュータと複数のストレージ装置が、スイッチを介して接続され、これらを統合管理する統合管理機構を備えたストレージエリア・ネットワーク・システムにおけるホストコンピュータであって、上記ホストコンピュータのストレージエリアネットワーク管理機構は、上記統合管理機構から通知されるストレージ装置に対する管理情報に基づきストレージ装置に対するアクセス情報を設定することを特徴とするストレージエリア・ネットワーク・システムにおけるホストコンピュータ。

(付記16) 複数のホストコンピュータと複数のストレージ装置が、スイッチを介して接続され、これらを統合管理する統合管理機構を備えたストレージエリア・ネットワーク・システムにおけるスイッチであって、上記スイッチの領域設定機構は、上記統合管理機構から通知される領域情報に基づき領域設定を行うことを特徴とするストレージエリア・ネットワーク・システムにおけるスイッチ。

(付記17) 複数のホストコンピュータと複数のストレージ装置が、スイッチを介して接続され、これらを統合管理する統合管理機構を備えたストレージエリア・ネットワーク・システムにおけるストレージ装置であって、上記ストレージ装置のストレージ管理機構は、上記統合管理機構から通知されるアクセス制限情報をに基づき、ストレージに対するアクセス制限条件を設定することを特徴とするストレージエリア・ネットワーク・システムにおけるストレージ装置。

(付記18) 複数のホストコンピュータと複数のストレージ装置が、スイッチを介して接続されたストレージエリア・ネットワーク・システムを統合管理する統合管理機構であって、上記統合管理機構は、ホストコンピュー

タのストレージエリア・ネットワーク管理機構に対して、ストレージ装置に対する管理情報を通知し、スイッチの領域設定機構に対して領域情報を通知し、ストレージ装置のストレージ管理機構に対して上記ホストコンピュータについてのアクセス制限情報を通知することを特徴とするストレージエリア・ネットワーク・システムにおける統合管理機構。

(付記19) 複数のホストコンピュータと複数のストレージ装置が、スイッチを介してファイバチャネルで接続されたストレージエリア・ネットワーク・システムを統合制御する統合管理プログラムであって、上記統合管理プログラムは、ホストコンピュータとストレージ装置とのアクセス経路情報に基づき、ホストコンピュータのストレージエリア・ネットワーク管理機構に対して、ストレージ装置に対する管理情報を通知する処理と、スイッチの領域設定機構に対して領域情報を通知する処理と、ストレージ装置のストレージ管理機構に対して上記ホストコンピュータについてのアクセス制限情報を通知する処理とをコンピュータに実行させ、ホストとストレージとのアクセス関係を一括して管理することを特徴とするストレージエリア・ネットワーク・システムを統合制御するプログラム。

(付記20) 複数のホストコンピュータと複数のストレージ装置が、スイッチを介してファイバチャネルで接続されたストレージエリア・ネットワーク・システムを統合制御する統合管理プログラムを記録した記録媒体であって、上記統合管理プログラムは、ホストコンピュータとストレージ装置とのアクセス経路情報に基づき、ホストコンピュータのストレージエリア・ネットワーク管理機構に対して、ストレージ装置に対する管理情報を通知し、スイッチの領域設定機構に対して領域情報を通知し、ストレージ装置のストレージ管理機構に対して上記ホストコンピュータについてのアクセス制限情報を通知し、ホストとストレージとのアクセス関係を一括して管理することを特徴とするストレージエリア・ネットワーク・システムを統合制御するプログラムを記録した記録媒体。

### 【0038】

【発明の効果】以上説明したように、本発明においては、S ANにストレージエリア・ネットワークを統合制御する統合管理機構を設け、ホストとストレージとのアクセス関係を上記統合管理機構により一括して管理するようにしたので、以下の効果を得ることができる。

(1) 信頼性の高い一元管理されたS ANシステムを構築することができる。また、前記したホスト・アフィニティ、ゾーニング等の機能を持っていない、過去のシステムに対しても対応できるので、全て新しいシステムを購入してS ANを構築することが動作環境の必須条件とならない。

(2) S ANの異常や、アクセスバスの整合性を容易に確認することができる。

(3) S ANを構成するホスト、HAB、スイッチ、ストレージ装置、FCA等が交換され、S ANの構成状態が変更されても容易に対応することができる。

(4) S ANに異常が発生した場合、被疑箇所やその影響範囲を容易に特定することができ、業務影響を最小限に止めることができる。

### 【図面の簡単な説明】

【図1】本発明の概要を説明する図である。

【図2】本発明の対象となるS ANシステムの構成例を示す図である。

【図3】本発明の実施例のS AN管理システムの構成を示す図である。

【図4】ストレージ装置のハードウェア構成例を示す図である。

【図5】アクセスバス設定情報、ストレージ・アフィニティ・テーブル、スイッチ・ゾーニングテーブル、ホスト・アフィニティ・テーブルの例を示す図である。

【図6】S AN統合管理機構が行う処理のフローチャートを示す図である。

【図7】ゾーニング設定機構が行う処理のフローチャートを示す図である。

【図8】S ANの障害管理を説明する図である。

【図9】障害報告方法定義の一例を示す図である。

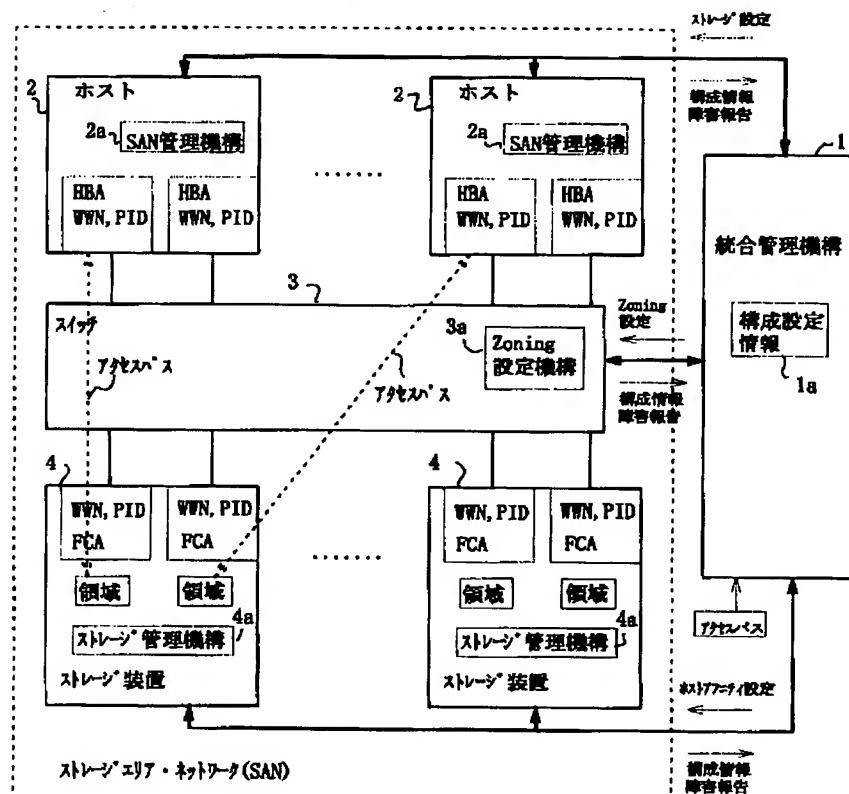
【図10】S AN統合管理機構が行うS ANの障害監視機能のフローチャートである。

### 【符号の説明】

1	統合管理機構
1 a	構成設定情報
2	ホスト
2 a	S AN管理機構
3	スイッチ
3 a	ゾーニング(Zoning)設定機構
4	ストレージ装置
4 a	ストレージ管理機構
1 1 0, 1 2 0	ホスト
1 1 1, 1 1 2	ホストバス・アダプタ (HBA)
1 2 1	ホストバス・アダプタ (HBA)
3 0 0	スイッチ
3 0 1	ゾーニング設定情報
4 1 0, 4 2 0	ストレージ装置
4 1 1, 4 2 1	ファイバチャネル・アダプタ (FC)
A)	
4 2 1	ファイバチャネル・アダプタ (FC)
A)	
4 1 8, 4 2 8	ストレージ管理機構
5 0 0	S AN統合管理機構
5 0 1	S AN構成設定情報

【図1】

## 本発明の概要を説明する図



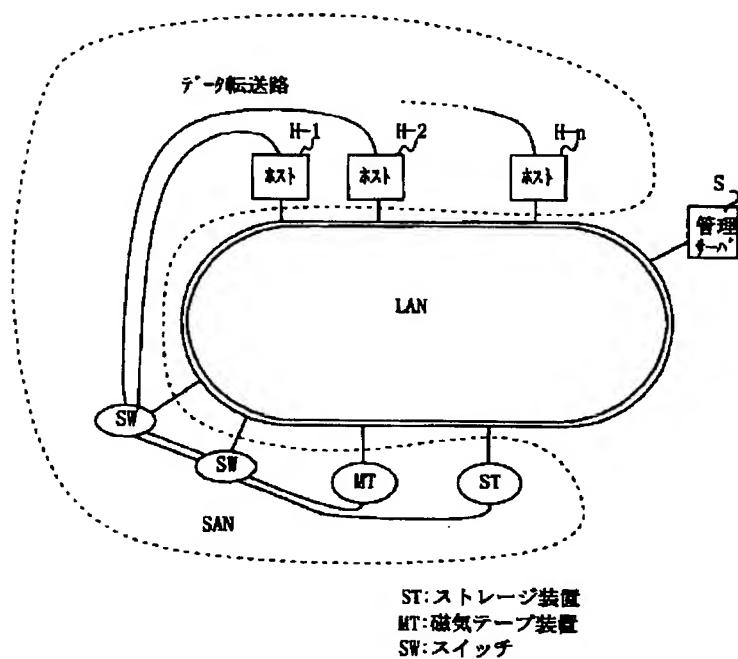
【図9】

## 障害報告方法定義の一例を示す図

受け取った障害情報	障害報告内容
FCA自己エラー+スイッチポートエラー+ホスト側アクセスバスエラー スイッチポートエラー+ホスト側アクセスバスエラー ：	FCA自己エラー スイッチポートエラー ：

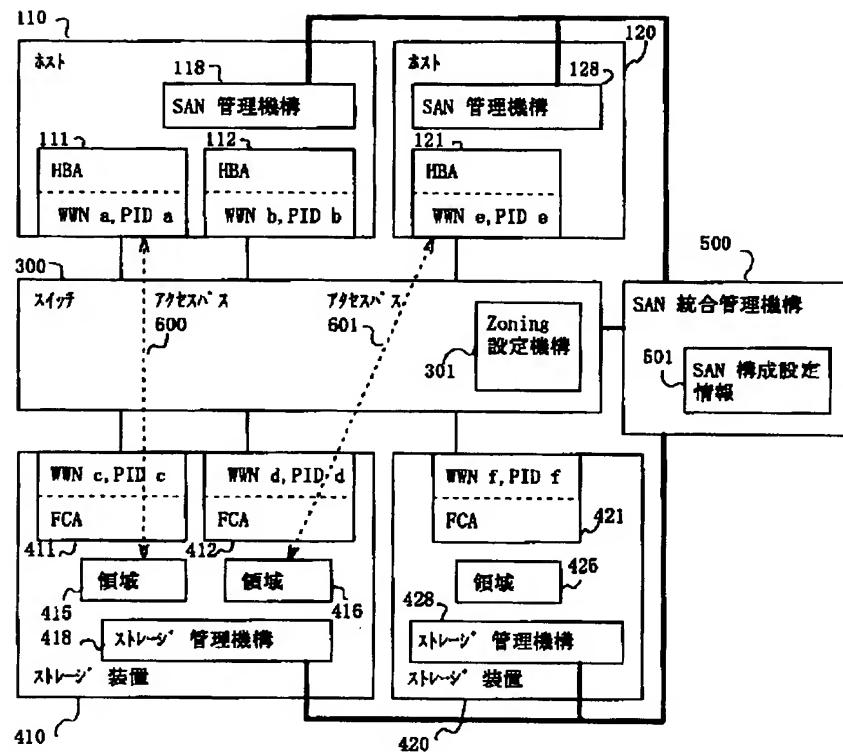
【図2】

本発明の対象となるSANシステムの構成例を示す図



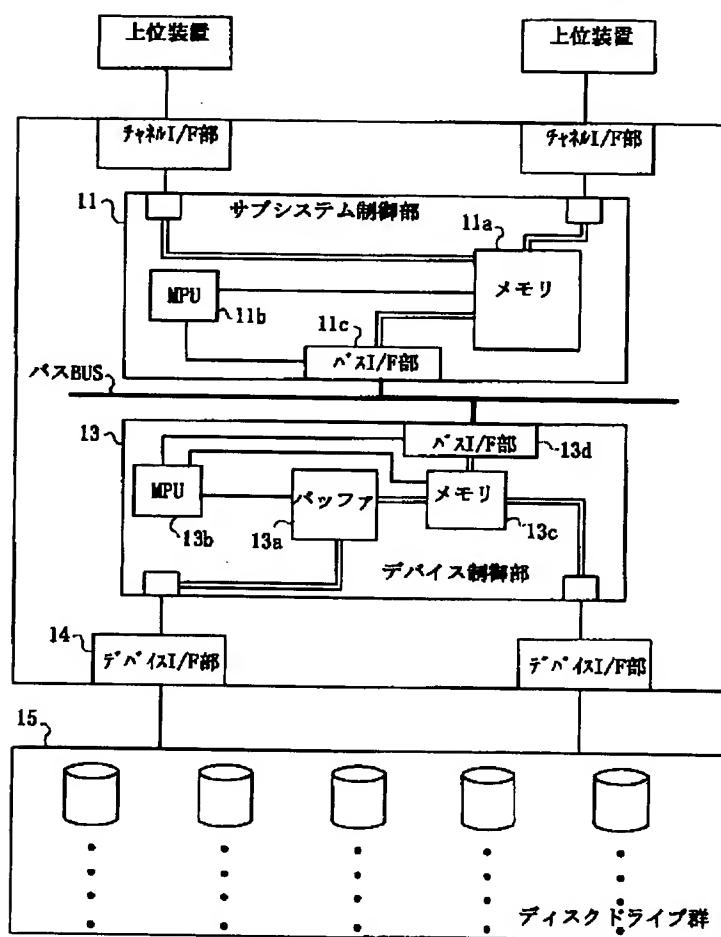
【図3】

本発明の実施例の SAN 管理システムの構成を示す図



【図4】

本発明の実施例のストレージ装置のハードウェア構成例を示す図



【図5】

アクセスパス設定情報、ストレージ・アフィニティ・テーブル、  
スイッチ・ゾーニングテーブル、ホスト・アフィニティ・テーブル  
の例を示す図

(a) SAN統合管理機構内のアクセスパス設定情報

アクセスパス	ホスト	HBA(WWN, PID)	ストレージ装置	FCA(WWN, PID)	領域
600	110	111(WWN <sub>a</sub> , PID <sub>a</sub> )	410	411(WWN <sub>c</sub> , PID <sub>c</sub> )	415
601	120	121(WWN <sub>a</sub> , PID <sub>a</sub> )	410	412(WWN <sub>d</sub> , PID <sub>d</sub> )	416

(b) Storage Affinityテーブル(ホスト110の場合)

HBA	アクセス先FCAの情報	FCA配下のアクセスする領域
111	WWN <sub>c</sub>	415
112	なし	なし

(c) Switch Zoningテーブル(スイッチ300場合)

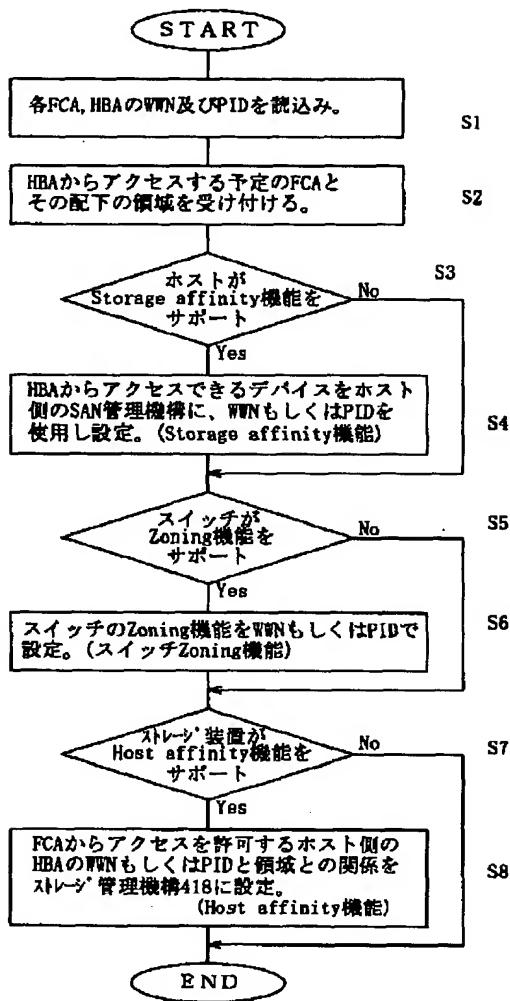
Zone名	Zoning設定
A	WWN <sub>a</sub> , WWN <sub>c</sub>
B	WWN <sub>e</sub> , WWN <sub>d</sub>

(d) Host Affinityテーブル(ストレージ410の場合)

FCA	アクセス許可HBAの情報	対応する領域
411	WWN <sub>a</sub>	415
412	WWN <sub>c</sub>	416

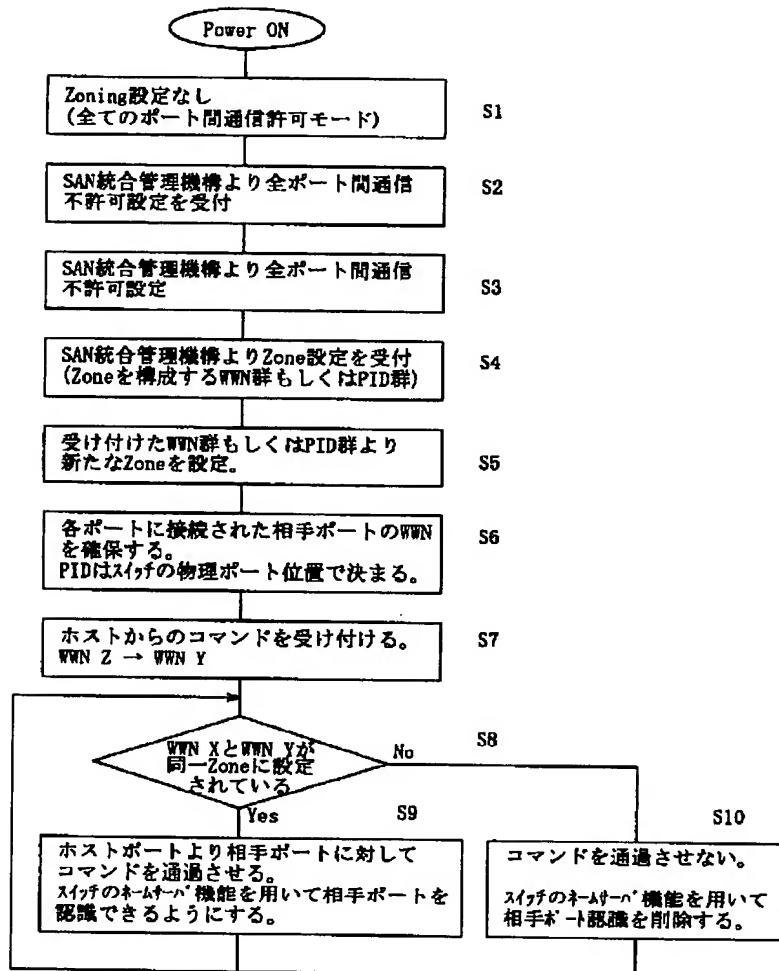
【図6】

## S A N 統合管理機構が行う処理のフローチャートを示す図



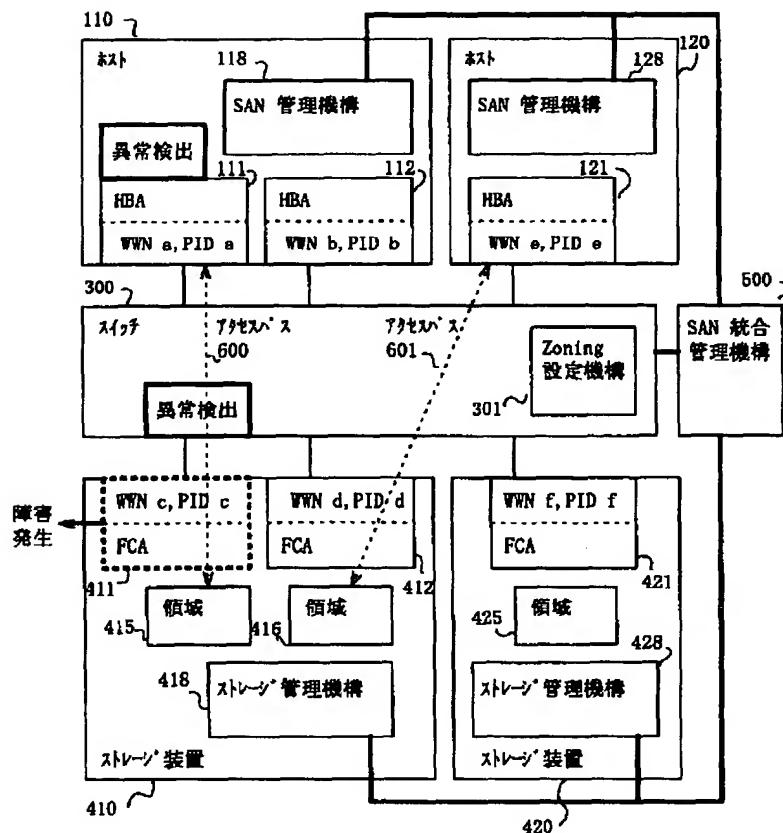
【図7】

ゾーニング設定機構が行う処理のフローチャートを示す図



【図8】

## S A N の障害管理を説明する図



【図10】

S A N統合管理機構が行う S A Nの障害監視機能の  
フロー チャート